UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/541,893	07/08/2005	Annegret Weng	DE03 0014 US	6238

65913 7590 03/12/2009
NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2437	
NOTIFICATION DATE	DELIVERY MODE
03/12/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	**Application No.** 10/541,893	**Applicant(s)** WENG, ANNEGRET
	Examiner MICHAEL PYZOCHA	**Art Unit** 2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _08 July 2005_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-20_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-20_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _08 July 2005_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _7/8/05_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending.

2. Preliminary Amendment filed 07/08/2005 has been received and considered.

Claim Objections

3. Claim 10 objected to because of the following informalities: “Cm” should be “CM” in order to maintain consistency. Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-17 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory “process” under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The method of determining a hyperelliptic curve including steps of selecting, determining and specifying is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent. Claims 18-20 recite an apparatus for using the method of claim 1. These claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the mean of 35 USC §101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims are rejected under 35 U.S.C. 102(b) as being anticipated by Weng ("Constructing Hyperelliptical Curves of Genius 2 for Cryptography, May 2002).

As per claims 1 and 18-20, Weng discloses selecting a CM field K (see page 2 step 1), determining a representant system of all isomorphism classes of simple principally polarized Abelian varieties having complex multiplication by the maximum order in K (see page 2 step 2), determining period matrices associated with the representant system (see page 2 step 2), determining theta-nulls (see page 2 step 3), determining class polynomials for the CM field over a finite field F_q (see page 2), determining a hyperelliptic curve over the finite field F_q and specifying the group order n of the divisor class group of the hyperelliptic curve (see page 2 steps 1-7).

As per claim 2, Weng discloses the hyperelliptic curve is of genus 2 (see page 2).

As per claims 3, 4, 5 and 6, Weng discloses the use of Igusa and Mestre invariants for the theta-nulls and to determine the class polynomials (see page 2 and sections 5-7).

As per claim 7, Weng discloses a plurality of suitable CM fields K and the associated class polynomials are stored in accessible form and a CM field is selected from the plurality help in store to determine the hyperelliptic curve (see sections 12).

As per claim 8, Weng discloses the period matrices are used in a Siegel-reduced form (see page 2).

As per claim 9, Weng discloses six theta-nulls are determined (see pages 2-10).

As per claim 10, Weng discloses to determine the representant system; a test is not made to see whether the fundamental unit of the real subfield of the CM field K is the norm of a unit of the CM field (see pages 2-10).

As per claims 11 and 12, Weng discloses a set of ideal classes is determined (see page 14).

As per claim 13, Weng discloses q is a prime number p (see page 2).

As per claim 14, Weng discloses the prime number p is selected such that each class polynomial has no more than h_k linear factors, where h_k is the class number of the CM field K (see page 2 and section 6).

As per claim 15, Weng discloses the CM field is selected such that the group order n of the divisor class group of the hyperelliptic curve is exactly prime (see page 2).

As per claim 16, Weng discloses q is the power of a prime number p (see page 2).

As per claim 17 Weng discloses keys are determined from the group of F_q-rational numbers of the hyperelliptic curve (see section 2.1 and section 12).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Examiner, Art Unit 2437